AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

Portland Division

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. '19 -MC- 129
The person of Paul Martin Rohlfing and the premises and outbuildings located at 2517 NW Neptune Ave., Lincoln City, OR 97367, described in Attachment A	)	

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Oregon *(identify the person or describe the property to be searched and give its location)*:

The person of Paul Martin Rohlfing and the premises and outbuildings located at 2517 NW Neptune Ave., Lincoln City, OR 97367, more fully described in Attachment A hereto.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before 3/6/2019 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Jolie A. Russo via the Clerk's Office .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 2/20/2019 11:00 AM

Judge's signature

City and state: Portland, Oregon

Honorable Jolie A. Russo, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Person and Place to be Searched

(1) The Person of **Paul Martin ROHLFING**, date of birth XX-XX-1974; and

(2) The Premises at **2517 NW Neptune Ave., Lincoln City, Oregon 97367** which is further described as a beige and brown two-story single-family residence with a rust-colored composite roof. The front door is brown and faces west. The black numbers "2517" appear on a white placard located north of the front door. There is an attached garage that faces west and is located next to the front door. A portion of the south facing wall is covered with wood siding. There is a brown staircase in front of the residence that leads to a second story door. A second staircase in the rear of the residence leads to a second story rear door. There is a small detached beige and brown building with a rust-colored composite roof located about 20 feet behind the main residence.

ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises located at 2517 NW Neptune Ave., Lincoln City, Oregon 97367 and the person of Paul Martin ROHLFING, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), transportation, receipt, distribution, possession and access with intent to view child pornography.

1. The items referenced above to be searched for, seized, and examined are as follows:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

c. Any and all motion picture films, video cassettes, and digital video disks ("DVDs") of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by United States mail or by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce (including by United States mail or by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs.

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, receiving, or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received, and the like.

i. Computers, storage media, or digital devices used as a means to commit the violations or that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, including transporting, receiving, distributing, possessing, and accessing with intent to view child pornography in violation of 18 U.S.C. § 2252A (a)(1), (a)(2) and (a)(5)(B).

j. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, web cams, microphones, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband, or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

k. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, iPods, iPads, tablets, and cellular telephones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been

created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to

determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.